Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)

Funded By U.S. Agency for International Development

Jordan e-Government Project

SGN Statement of Needs

Final Report

Deliverable for ICTI Component, Task No. 431.4.2
Contract No. 278-C-00-02-00201-00

June 2002

This report was prepared by Paul Williams, in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan.

0 Document Control

Table of Contents

TABLE OF FIGURES

0.1 Document History

Version	Status	Reviewed/Approved by	Date
V0.1a	Draft	Alistair Hodcroft, Paul Maclean	29th May 2002.
V0.1b	Draft	Deema Anani, Abed Shamlawi	10th June 2002
V1.0	Final		

0.2 Changes From Last Issue

Version	Date Updated	Revision Author	Summary of Major Changes Made	Reviewed By	Review Date
V0.1b	18/06/02	P Williams	Review Comments included		

0.3 Acknowledgements

N/A

0.4 Distribution List

Allan Gormley	EDS
Kendall Lott	EDS
Mahmoud Ali Khasawneh	MoICT
Reg Miller	AMIR
Abed Shamlawi	AMIR

0.5 Referenced Documents

Reference Number	Title	Note
1.	The Hashemite Kingdom of Jordan e-government Blueprint & Roadmap (version 5, 12th September 2001).	
2.	Email Statement of Needs GOJ.CONS.ANLS.028.0.2	
3.	Web Applications Assessment GOJ-CONS-ANLS-025-0.4a	

0.6 Abbreviations

COTS	Commercial Off The Shelf (a software package)
ERP	Enterprise Resource Planning
DMZ	Demilitarised Zone
DNS	Domain Name Service
GOJ	Government of Jordan
G2B	Government to Business
G2C	Government to Citizen
GSI	Government Secure Intranet (see the entry for SGN in the glossary)
LAN	Local Area Network
MIB	Management Information Bases
MoICT	Ministry of Information & Communications Technology
MoPC	Ministry of Post and Communications (the previous name of MoICT)
NIC	National Information Centre
NMI	Non-Ministerial Control Institution
OGD	Other Government Department
PC	Personal Computer
SGN	Secure Government Network
URL	Uniform Resource Locator – the official term for a web address such as www.nic.gov.jo

0.7 Glossary

This section defines the following terms that are used in this report:

CAT-5	Category 5 describes network cabling that consists of four twisted pairs of copper wire terminated by RJ-45 connectors. Cat-5 cabling supports frequencies up to 100 MHz and speeds up to 1000 Mbps. It can be used for ATM, token ring, 1000Base-T, 100Base-T, and 10Base-T networking.
DMZ	A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defence, usually some combination of firewalls.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Internet - also known as the World Wide Web (www)	A worldwide network of linked PCs. Information is published to the public in graphical format on Internet Web sites for anyone to view. Many national governments now have one portal site to which users are initially directed, before being redirected (often by a search engine built into the portal) to the Web site of the government department that they are seeking. (For an example, see www.ukonline-Gov.uk)
LAN	A network, restricted to government users, which links PCs within a ministry. It uses protocols such as Token-Ring to share electronic files around the LAN. The format of these files is generally limited and will not usually include the graphical and enhanced formats that are available on an intranet.
Portal	A front-end software component that is provided on the Internet and on intranets (such as the SGN) to make it easier for users to find information and services. There are many components of a portal but the most important ones include a content management system (to ensure that the information content is of high quality), a search engine (to help the user find the information content that is of interest to them), and a directory of users.
Secure Government Network	An intranet that is provided by a government for the exclusive use of its civil servants. It will be provided with high levels of security to prevent any non-government users from gaining access to it. This type of network is also known as a Government Secure Intranet (GSI). Each Ministry will probably have its own intranet Web site that will provide information to intranet users.

1 Introduction

1.1 Objectives

This report has been produced at the request of the Jordanian Government. It is the result of a review of the Network Needs of e-Government. This document is intended to form the basis of a Secure Government Network design proposal (SGN Design) or a Request For Proposal (RFP).

In this document the term 'Institution' is used to describe all physically distinct GOJ (Government of Jordan) institutions, be they officially categorised at Ministries, Departments, Institutes, Municipalities, or otherwise.

1.2 Sources of Information

The information for this report was gathered during two trips to Jordan between March and May 2002. The institutions used to gather the information may be divided into Ministries, Government Departments and those institutions not under direct ministerial control (NMI). These institutions are shown in Figure 1 - Possible Connections to SGN. The full list is as follows:

1.2.1 Ministries

- Ministry of Information & Communication Technology (MoICT)
- Ministry of Industry & Trade (MIT)
- Ministry of Planning (MoP)
- Ministry of Public Works & Housing
- The Prime Ministry (PM)
- Ministry of Finance (MoF)

1.2.2 Government Departments

- The National Library
- Department of Statistics (DoS)
- Department of Social Security (DSS)
- Customs Department

1.2.3 Non Ministerial Institutions

- The Municipality of Greater Amman (MoGA)
- Jordan Capital Markets (JCM)
- Jordan Industrial Estates Corporation (JIEC)
- Jordan Investment Board (JIB)
- Jordan Export Development and Commercial Centres Corporation (JEDCO)
- Central Bank of Jordan (CBJ)
- National Information Centre (NIC)
- Aqaba Special Economic Zone Authority (ASEZA)

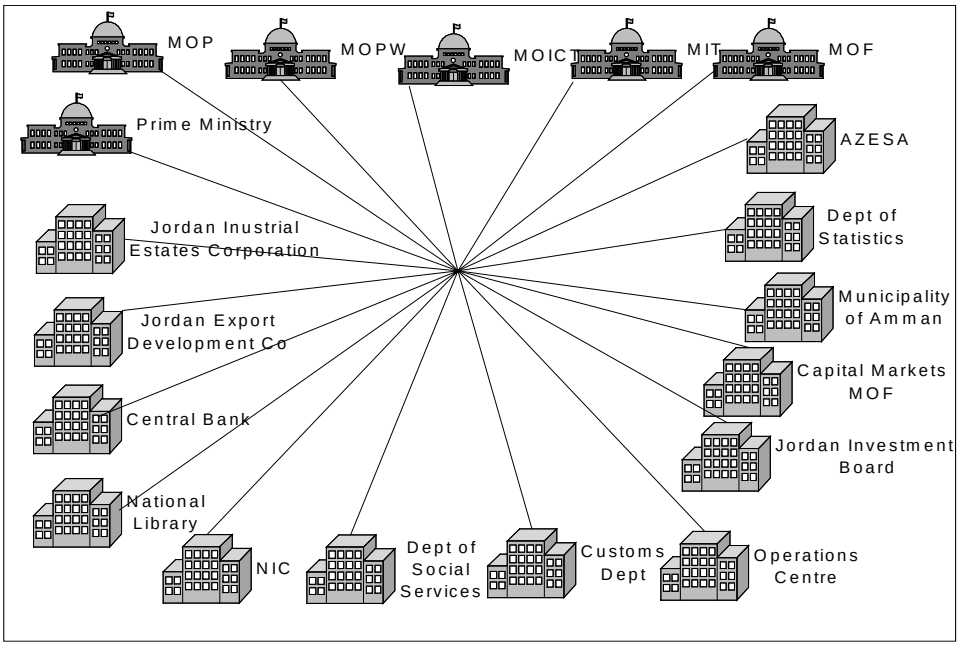

Figure 1 - Possible Connections to SGN

Information was gathered by the author during interviews at these GOJ institutions, was written-up, and then sent back to the relevant interviewee for validation, in order to ensure its accuracy.

The following institutions were also visited during the information-gathering phase to determine potential sites for the e-Government Operations Centre.

- National Information Centre (NIC)
- Jordan Telecom Company (JTC)
- Central Bank of Jordan (CBJ)

In addition to visiting the organisations specified above, a number of documents were used extensively for reference purposes. These are specified in section 0.5

1.3 Acknowledgements.

The findings, conclusions and recommendations in this report are based directly on information provided to the author by the documents specified above and by the following individuals during discussions. The author should like to express thanks to the latter for finding the time, and to those of them who subsequently validated the meeting notes.

- Jamil Al-Amleh — Head of the IT Department, Municipality of Greater Amman
- Najeh Mohid Al Saied — IT Department, Municipality of Greater Amman
- Mohamed Ayed Abu Asal — Assistant Computer Director, Ministry of Industry & Trade
- Mazen Amarin — Consultant, National Information Centre
- Rula Bayazed — Head of Computer Department, Prime Ministry
- Mamoun Th. Talhouni — Secretary General, National Library
- Yousef F. Goussous — Information & Computer Director, Min. Public Works & Housing
- Sana Halabi — Information Manager, Legislation Office, Prime Ministry
- Atif Hamdan — Director of IT, Ministry of Industry & Trade
- Jamal I Q Issa — Manager, Computer Department, Central Bank of Jordan
- Marwan Abu Sara — Ministry of Public Works & Housing
- Abdel-Rahman Shihab — Director, Computer & Information Directorate, Min. Planning
- Fadhl Sweedan — Director, Technical Services, National Information Centre

- Tariq Taqieddin — Network Administrator, Information Dept, Prime Ministry.
- Atef I. Abed Al-Rahman — IT Director, JEDCO
- Raed M. Dummor — IT Manager, JIEC
- Rasheed Al-Nahlawi — IT Manager, JIB

The author would also like to thank the following for input, advice and assistance:

- Mahmoud Khasawneh — Chief Information Officer, MoICT
- Reginald Miller — ICT Component Leader, AMIR
- Deema Anani — Advisor, Policy & Strategy, MoICT
- Rula Barghouty — Technology Advisor, MoICT
- Roger Guichard — Advisor, Policy & Strategy, MoICT
- Abed Shamlawi — ICTI Technical Advisor, AMIR

I am also grateful to Mr Firas Numan Rsheidat (E-Gov Co-Ordination Unit, MoICT) and Mr George Abedrabbo (AMIR) who accompanied me on several of the meetings and who provided Arabic-English translation when needed.

2 The Current Network Infrastructure

This chapter summarises the detailed notes contained in Appendix A. It describes the network and hardware that is currently in place in the aforementioned GOJ Institutions. Information regarding applications at each institution may be found in document Web Applications Assessment GOJ-CONS-ANLS-025-0.4a Reference 3.

2.1 Ministry of Information and Communications Technology (MoICT)

2.2 Ministry of Industry & Trade (MIT)

2.2.1 Staff and Equipment Summary

The Ministry comprises 11 district offices and the HQ building in Amman. These are linked by a WAN via 12 leased lines, with about 120 users connected in the district offices.
All of the Ministry's 500 networked users are provided with email and it is used widely.

Six floors of the HQ building are connected to a LAN, all cabling being to CAT5 standard (capacity up to 100 MB/Sec.). About 380 users are connected to the LAN. The Ministry has 10 servers, the main one being a Sun Ultra 3000 to which the whole Ministry is connected. The Ministry also runs its own Web server, firewall server and mail server. A further Bull machine is reserved for e-Government use.

The system uses TCP/IP with fixed IP addresses (only 64 currently allocated) but the only intranet application in use at the moment is the Company Registration system (see below).

About 150 of the Ministry's staff have access to the Internet and they make extensive use of it for research.

2.2.2 Other Information

The only Web application currently in 'live' use is the Web site (www.mit.gov.jo) – a new version (with a link to the on-line Company Registration system) of this will go live once the Internet connection into the Ministry has been expanded from 64kbps to 512kpbs (this is due to happen by April 2002).

2.3 Ministry of Planning (MoP)

2.3.1 Staff and Equipment Summary

About 180 of the Ministry's staff are equipped with PC's, which are fully LAN connected and have access to the Internet. This network operates with traditional LAN protocols rather than TCP/IP – it is not an intranet.

They are connected to the NIC via a 56K leased line (due to be upgraded to 512k in the near future). Another server is to anti-virus detection.

All the Ministry's PCs are equipped with email but this is not widely used. The reasons for this were defined as:

- Computer literacy is low
- Staff have not yet adopted a mind-set to use email
- Staff are unfamiliar with the technology.

2.3.2 Other Information

The provision of appropriate and sufficient training (both general training in PC literacy and specific email training) will be the key to persuading GOJ civil servants to start using email in their daily work. The email training should include classroom courses (specific functionality and etiquette) and informal workshop events (to demonstrate the benefits of email to those whose computer literacy is not yet highly developed).

Access to the Web is rationed and depends on an individual's position within the Ministry (some staff have 2 hours access in the morning and afternoon, others have all-day access).

2.4 Ministry of Public Works & Housing

2.4.1 Staff and Equipment Summary

The main Ministry building in Amman has a LAN that connects about 40 users. Currently only the following departments are connected to the LAN:

- The Financial Affairs Dept
- The Personnel Dept
- The Administrative Dept.

Outside Amman there are 12 district offices that are connected through a WAN (dial-up connections) to MPW head-office for file transfer etc. Internet protocols are not yet used on this network so there are no intranet applications in use at the moment.

2.4.2 Other Information

A limited number of staff are equipped with email but it is not used widely – this is partly because MPW does not receive many email messages from OGDs (Other Government Departments). The Ministry's email server is hosted by the NIC and staff dial-up once or twice each day to get their email.

There are about 3 or 4 stand-alone PCs connected to the Internet and used for general research purposes through the standard Internet search engines. There are no other Web applications in use.

The MPW Internet Web site (www.mpwh.gov.jo) is currently hosted by the NIC. This is a static site, providing a considerable amount of information content in Arabic and no transactional functionality, but there are plans to upgrade this.

2.5 The Prime Ministry (PM)

2.5.1 Staff and Equipment Summary

The Prime Ministry (PM) supports the office of the Prime Minister and is located in three buildings on one site. The buildings are linked by an ATM backbone and are connected to NIC. There are about 120 network users on site. There is no intranet. About 90 network users are provided with direct access to the Internet

2.5.2 Other Information

All networked users have access to e-mail – however, email is not widely used because there is a manual mail service that sends paper notes around the site.

The Web is used for general information gathering.

2.6 Ministry of Finance (MoF)

2.6.1 Staff and Equipment Summary

MoF has 5 Directorates within AMMAN. These are currently not connected but an IT network has been tendered. The intention is to implement the network in stages:

- Stage 1 - Intranet – Connect via WAN
- Stage 2 - Extranet – Income Tax and Land Service
- Stage 3 - Intranet – Public Access.

The intention is that in the future citizens will be able to pay their taxes at any directorate office.

There are 34 Directorates that collect taxes across Jordan. A WAN to connect each of the branches with the main building (the Operations Centre) is planned, with the initial intention being to connect 8 directorates this year and then more at a later date.

2.6.2 Other Information

MOF has close relations with MoP and the Central Bank of Jordan. There is a leased-line connection between MoF and the Central Bank that is used to exchange commercial information and financial data.

A very small number of email addressees currently exist – all staff that need to use email use private accounts such as Hotmail.

The systems online at present are financials, expenditure, payroll, personnel and a tax system.

Internet Connection is currently through the NIC who publish a static website (www.mof.gov.jo) for the Ministry. A new website is currently being developed in-house.

2.7 The National Library

The national Library is part of the Ministry of Culture.

2.7.1 Staff and Equipment Summary

AMIR have provided 6PC's P1-P11 and an HP Rs3000 Server. The system uses HP system MPE XL and the programs developed use a MINISIS database. The storage capacity is 20Gbytes. They estimate that they need at least 100Gbytes. ***It is recommended that they need at least 200Gbytes.***
There are 6 IT personnel. They will require further training allowing them to form part of any e-Government structure. The web site is at www.nl.gov.jo, hosted internally with NIC as ISP. The site will be officially launched in the immediate future.

2.7.2 Other Information

The building that houses the library is very old and seems to be inadequate for this purpose. A significant shortage of space means that much of the library and copyright material is in storage boxes filling 3 rooms. The building is 2,500 sq ft; a more realistic size would be c. 15,000 sq ft. There have been previous requests to be relocated and it is hoped to do so as soon as is feasible.

They have developed a system to allow cataloguing of the books by title, author, classification and a brief description (a bibliography). Information is entered by a clerk who scans in the documents. This is a very small scanner and is not suitable for any large-scale operation. It would be extremely useful if there was some form of OCR equipment. The web site will allow searching of this information and brings back all pertinent documents. A second system allows registration of copyright information. This will also be available via the web site.

The department has responsibility for Copyright protection and enforcement. Six Inspectors have the power to investigate any organisation in Amman and to confiscate counterfeit goods. They can send information to the Ministry of Justice requesting prosecutions. They are also called by customs officers stationed at Queen Alia Airport and at border stations to check goods that are being imported. They have the power to stop entry or let them through.

These processes are all done via phone calls and paper communications. This makes the status of prosecutions for example very difficult to track. The department would like electronic communication with tracking /mechanisms.

This department contains a wealth of cultural information (books, CD's, photographs) about Jordan and would be a useful component for any GOJ E-Government initiative. This department is a potential reference site that would provide users with access to a diverse range of information so it may be prudent to upgrade its facilities.

2.8 Department of Statistics (DoS)

2.8.1 Staff and Equipment Summary

The department has 400 Employees and is located in two buildings that are situated on one site
There are 200 PC's, 37 dumb terminals (for data entry only). These PC's are a combination of windows 98 and windows 2000.
The department has 70 IT Staff including data entry personnel and 2 Network specialists.
A Switched network LAN/WAN is in use connecting 200 users.

There is a Dialup connection to Customs Department.
The department has 8 servers (Sun Servers (6 Servers), NT Servers (2 Servers)) all contained within a dedicated computer room.

2.8.2 Other Information

The department uses one Application, which is Oracle based (Developer 2000 and Forms 30).
The web site address is www.dos.gov.jo hosted at the site itself, using the NIC as ISP.
All staff make minimal usage of the Internet.
The email system in use is a combination of Send Mail and Hotmail for personal E-mails

2.9 Department of Social Security (DSS)

2.9.1 Staff and Equipment Summary

There are 900-1000 staff within the department, split across 16 Branches.
There are 30 Staff in the IT department, including 16 Programmers, 3 Hardware support, 3 DBA's and 3 Data Entry Clerks.

Main equipment is a digital Alpha 8200 Unix system. Running legacy systems on Oracle 8. They have RAID disk storage of 40Gbytes.
The web site and applications server is a mid range Compaq machine.

2.9.2 Other Information

They have 22 in-house built systems. The systems include administration, HR Personnel, Payroll, Financial systems (reconciliation, settlements etc) registration of employees. These are dumb terminal entry systems.

All payments and requests for payments are made on a face-to-face basis and entered via terminal systems. (Plans are in progress to develop their own e-payment system with the Arab Bank)
Only Internet mail is used at present and seems to be limited to about 20PC's
Current implementation includes:

- Replacement of the existing systems with Internet enabled Oracle systems.
- Development of a document management and workflow system.
- Development of an archiving system
- Plans are in place to have a new system (fast track e-services) which will allow online registration of employees, changing of jobs and querying personal details.

Leased lines are in place from the branches 64K rising shortly to 128K. These are all connected to the Alpha machine.

All paperwork and files are held within the local branches. This means that it takes up to 2 weeks to get the information back to head office.

Registrators must have an account with the ARAB Bank. Payments must be made to the account and this payment gets transferred automatically to the departments account.
This registration is not the same ID as the registration within the MIT.

They receive a CD every fortnight from the civil statistics bureau of national ID's. This is used to cross-refer to the social services ID.

The website is at present a static website using CNS as an ISP.

2.10 Customs Department

The Customs Department is part of MoF. It has border posts at all the road entries to the kingdom and at Queen Alia Airport, an HQ building in Amman, and various other stations and warehouses around the country. There are about 10 facilities in the Amman area.

2.10.1 Staff and Equipment Summary

The Customs HQ building in Amman is provided with a LAN, an email system and about 60 Internet users. There are 17 directorates in the Customs Department, all of which are equipped with PCs but email is not yet widely used between them.

2.10.2 Other Information

The HQ building is linked to most of the Customs facilities by a satellite network through a fibre-optic link to the Hashim-1 satellite dish at the Jordan Telecom facility in Amman. The satellite network carries video, voice and data traffic. Most of the border posts are also provided with leased-lines that are used for data transfer or as a backup communications network.

The Customs Department HQ is equipped with email but apparently only the staff in the HQ building use it. The Customs Department has an Internet Web site at www.customs.gov.jo

2.11 The Municipality of Greater Amman (MoGA)

2.11.1 Staff and Equipment Summary

The Municipality of Greater Amman (MoGA) provides municipal services to the citizens of Amman. The majority of these services are delivered in face-to-face meetings when the citizen visits MOGA offices - either the main office building in the centre of the downtown part of the city or 30 (approximately) district offices in the suburbs of the city.

The main office is a modern complex of buildings that is equipped with a LAN that currently links about 200 users who are provided with PCs and dumb terminals. About 20 of the district offices are connected by leased-line to the main office building. MoGA hosts its own network server. There is no intranet in use at the moment.

2.11.2 Other Information

Most of the staff connected to the network are provided with email and appears to be widely used. However there appears to be only a limited number of external email addresses (such as mogamman@go.com.jo) in use.

The Internet is used for general research by MoGA staff. Staff are only given access to it if a business need exists. MOGA hosts its own Web server.

2.12 Jordan Capital Markets (JCM)

2.12.1 Staff and Equipment Summary

Jordan capital markets (JCM) is made up of 3 institutions. Amman Stock Exchange (ASE), the Jordan Securities Commission (JSC) and the Securities Depository Centre (SDC). The ASE and SDC offices are situated in the brand new JMC Building. This building has a LAN with a number of sub-networks to accommodate the existing applications. There are 2 computer rooms equipped with UPS and fire protection. JSC is situated in a separate building name the housing centre. This building also has a LAN again with various sub-networks. The 2 buildings are connected with a fibre-optic cable switched to form a single LAN across both buildings.

The ASE network has to support 35 certified broker companies. The SDC network requires these same companies with an additional 300 issuing companies (dialup links), 15 custodians and the settlement bank (leased lines). JSC has a requirement for 52 staff.

There are approximately 150 staff contained within these buildings.

2.12.2 Other Information

Internet connection is via Global One.

This 'institution' has been heavily funded and as such a whole host of equipment is contained within these buildings. Furthermore numerous plans and strategies are in place to expand and consolidate the current structures. This includes firewalls, email systems etc. A DMZ is already in place within ASE.

This information, although available for analysis purposes, has not been included in this document.

In terms of connection to the SGN the capital markets should be one of the 'smoother' transitions.

2.13 Jordan Industrial Estates Corporation (JIEC)

2.13.1 Staff and Equipment Summary

The JIEC comprises 3 locations. The main site location which houses 80 staff members is in Amman. There are 2 remote sites that have a leased line link to the Amman site. These are Irbid and Kerak. These sites have approximately 10 staff members combined. They also have dial up users.

The current email system is Artesoft but they will be implementing Exchange 2000 within the month, when their ISP connection is installed. The email client will be Outlook 2002 (Office XP). There are 15 Windows 2000 machines, 20 Windows 98 Machines and 60 Windows 95 machines. They currently have 5 Servers: 1 Proxy server, 1 web server, 1 Database server; 1 Active directory W2K server and 1 Exchange 2000 server. The promotions department is the heaviest users of email. This department consists of 20 users

JIEC has 3 IT staff Members comprising 2 programmers and 1 System Admin.

2.13.2 Other Information

JIEC does not have any direct WAN connections to any Ministries. They communicate heavily with MIT.

JIEC's ISP is Global One. They are waiting on a 128kb link to be installed.
JIEC's web sites are www.jiec.com.jo and www.jiec.com. They do not have any web-based applications. They have about 25 database applications that they would like to bring to the WEB. A company called CNS hosts their web site.

2.14 Jordan Investment Board (JIB)

2.14.1 Staff and Equipment Summary

The JIB comprises 2 locations. The major location which houses 80 staff members will be moving to a new location within a couple of weeks. The second location is one terminal at the Amman Airport. The airport location has a couple of staff members. Of the 80 Staff members residing in the main location 70 are LAN users, all have email access (25 users as medium to heavy email users), and 25 have INTERNET access.

The current email system is Exchange 2000. The email client being used is Outlook 2002 (Office XP). The majority of the client machines are Windows 2000. Exchange 2000 sits on top of a Windows 2000 Active Directory infrastructure. This infrastructure consists of 3 servers: 1 Active Directory domain controller/ISA server; 1 Active Directory Global Catalogue/ Fax Server; and 1 Exchange 2000 server. The Fax Server is Fax Maker, which receives Faxes and routes them to a printer. The promotions department is the heaviest users of email. 90 % of their work is through email.

JIB has 4 IT staff Members comprising 3 programmers and 1 System Admin.

2.14.2 Other Information

JIB does not have any direct WAN connections to any Ministries. They communicate heavily with MIT.

JIB's ISP is NetsOnline. Their new Location will have a 256KB link.

2.15 Jordan Export Development and Commercial Centres Corporation (JEDCO)

2.15.1 Staff and Equipment Summary

JEDCO consists of 1 site with 50 LAN. The LAN is currently 10MB speed but will be upgraded to 100 MB this year.

The current email system is SUN SendMail. The email client being used is Outlook Express. The majority of the client machines are Windows 98 and Pentium I. They have 4 Windows 2000 PCs. JEDCO has 3 servers: 1 Database Server – Oracle 8I (Digital); 1 WEB/EMAIL Server (SUN); and 1 firewall server (SUN). Their email address is user@jedco.gov.jo.

JEDCO has 5 IT staff Members comprising 3 programmers, 1P.C. Tech and 1 Director.

2.15.2 Other Information

JEDCO does not have any direct WAN connections to any Ministries. They communicate heavily with MIT.

JEDCO's ISP is Global One. They have a 128 Kb leased line.
JEDCO's web sites are www.jedco.gov.jo, www.iop.jedco.gov.jo, www.atp.jedco.gov.jo, www.agreements.jeco.gov.jo, and www.ean.jedco.gov.jo. They also have an intranet where they have some workflow type applications, such as leave request.

2.16 Central Bank of Jordan (CBJ)

2.16.1 Staff and Equipment Summary

There are currently about 700 users with 43 staff in the IT department (of which 20 are IT staff and 23 administration and management). About 650 PC's and dumb terminals (with text emulators) are connected (using various operating systems).

Hardware currently in use includes:

- Digital alpha 8200*2
- 4 Compaq Ds40s (2 with 2 CPUs + 1Gb RAM, 2 with 1CPU + 0.5Gb RAM, and a total of 400 Gbytes of disk space)
- IBM Firewalls

The system comprises two main networks and several smaller interconnected networks (e.g. Novell is used for library and internal applications). The internal network is based on a star topology with CAT-5 and fibre optic links within the computer room. Another network is frame relay.

Cabling is Fast Ethernet LAN and fibre-optic with 2Mb Fibre-optic connection to NIC.

CBJ have an impressive and professional standard Computer room with the following features:

- fully secure (centrally located on the first floor behind locked doors)
- CCTV monitoring
- Air Conditioning
- Raised Floors
- Insect and flood protection
- Anti-static and Dust paint on walls
- Full UPS controlled from outside
- Automatic/semi-automatic/manual alarm system
- Halon-flood fire protection (sourced from a separate room)
- Emergency battery backup (in a separate room)
- Standby generators are in the basement
- Machines controlled from inside and outside computer room
- Data backups are taken weekly and deposited at the University.

A backup system is situated at the bank's clearing house in a separate building (100 metres down the road).

All systems allow for dial-up access..

2.16.2 Other Information

The bank has many applications. These have been developed in the past using Cobol and RDB (running on the Alphas). Current applications are being developed using Designer 2000 and Oracle 8i.
Main development at the moment is RTJ. This is a real time gross settlement system. This system will run on a connected network of 22 banks connected to the central bank. All hardware and software will be housed at the central bank. The system will be built using SWIFT (a secure payment system). The system will allow credit validation, transaction moving and clearing facilities. It will be an online Internet based system. SEMA are doing the implementation, which will be phased (13 Banks will be connected initially, with international banks at a later date).
This system will be implemented within the 2nd/3rd Qtr 2002.

The bank's IT department are currently developing interfaces to this new system.

Other applications include HR, Personnel systems, Payroll, risk management, credit health checking. Clearing system (reconciliation/settlement)

At present there is no direct lines between other international banks.

The bank has a self-built website www.cbj.gov.jo. The main ISP is NIC. This is via a 2mb fibre optic link. Currently using 512Kb, but can ramp up immediately depending on usage. Some of the branches use different ISPs. This site contains published information on statistics and reports. E.g. Reuters/ Bloomberg information, exchange rates.

The bank uses Microsoft exchange as its email system.

2.17 National Information Centre (NIC)

2.17.1 Staff and Equipment Summary

The National Information Centre, in addition to be the owners of the master DNS service within Jordan, provides an Internet Service to the majority of government institutions within Jordan. These are in the main leased lines between the NIC and the connected institutions. The NIC provides limited web hosting and backup email services. The NIC is connected directly to the RJAF fibre-optic network, which is scaleable to 2Mb. This network is currently used to connect the University of Jordan and the Central bank.

The NIC has 36 IT staff covering a wide range of hardware, software and consultancy skills. The NIC web site acts as a guide to the content and information contained in all the other connected web sites. Links are available to each of the web sites supported. The web site also includes statistical information compiled by the NIC on Jordan.

2.17.2 Other Information

The NIC administers the construction, implementation and the training of staff for the JITTC community centres. These have potential in the long term to provide access to the SGN. Due to the services already offered and the potential for the upgrading of their system, the NIC should be considered as a potential site for the e-Government SGN Operations Centre.

2.18 Aqaba Special Economic Zone Authority (ASEZA)

ASEZA is a free zone with reduced taxes and no custom duties.
Companies and shops etc are awarded licences to work within the free zone.
ASEZA communicate in paper form with JIEC, JIB, JEDCO and the tourist board. Although part of the customs department there are no electronic connections between ASEZA and the rest of Jordan.

2.18.1 Staff and Equipment Summary

There are 130 PC users out of 400 employees. 200 users will be connected eventually. Each user has a Pentium III pc with windows 2000 professional. The IT department consists of 1 person.

The organisation is contained within 2 buildings. One contains 5 servers and the other just one. A fibre-optic link connects both buildings. 10/100Mb Ethernet is installed.
The buildings house 6 servers (Exchange server, Two printer/file servers, Shared Sever, Database server and a Standby server)

There is no Internet connection.

2.18.2 Other Information

No systems run on the network. The PCs are primarily used for word processing and email. The email system is Microsoft exchange 2000. A dialup connection exists through a proxy server and router. A firewall exists on the router. Microsoft checkpoint is installed but not currently running.

2.19 Jordan Telecom Company (JTC)

2.19.1 Overview

Jordan Telecom company (JTC) is a partly state owned monopoly that offers a full range of analogue and digital based communication services throughout the whole of Amman and in most parts of Jordan.

2.19.2 JTC Network

The SGN will utilise the JTC ATM backbone.
Figure 2 Shows the existing ATM backbone that will be used for connecting the various institutions. This backbone is controlled by a series of switches and routers maintained by JTC. The configuration and responsibility for this equipment rests with JTC.

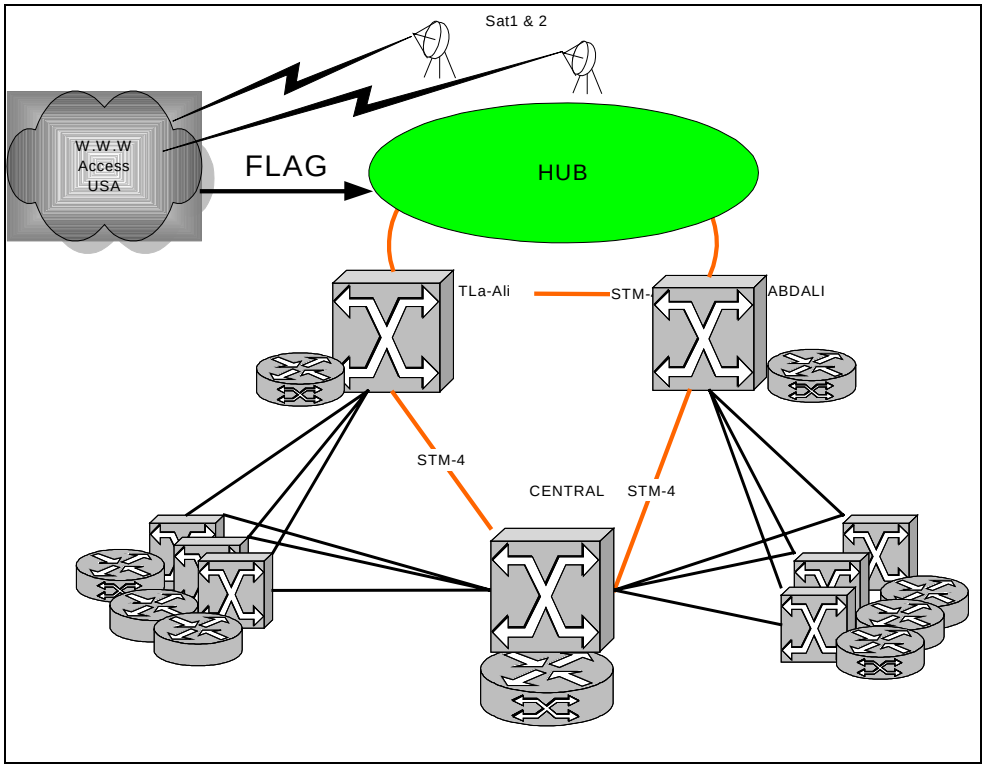

Figure 2 JTC ATM Network Architecture

3 Functional Requirements

3.1 Requirements Scope

The Government of Jordan is seeking to implement a Government wide network infrastructure, to be known as the Secure Government Network (SGN) that will eventually link all government institutions. The SGN will enable secure Department-to-Department interoperability and interconnectivity, support secure connectivity to the Internet and provide the mechanism for introducing Government wide shared services accessible by all Departmental users.
The SGN must be scalable to eventually allow Government-to-Business (G2B) and Government-to-Citizen (G2C) interoperability.

The approach that will be adopted to deliver this infrastructure is to have the physical networking component provided by the local telecommunications provider JTC. JTC will provide all the cabling network infrastructure up to and including the 'wall port(s)' within the targeted Department Offices. The second 'layer', the subject of this Statement of needs, will provide the secure, managed connectivity between the SGN, the Institutions network(s) and the Internet.

3.1.1 SGN (Router / Firewall access):

The SGN will be based on a public ATM (Asynchronous Transfer Mode) network with ATM access points located at each Government department. The public ATM service is provided by JTC. Each department must be protected, using a firewall solution, when accessing the SGN. This standardized, single IP backbone will provide the required business services including: email, Internet Access, Any-to-Any communication as well as connection to external entities (like the private sector) and the public (over the net).

To assure the availability of this 'layer' it is recommended to incorporate a fully functional e-Government Operations Centre. This Operations Centre will manage the day to day running and availability of the Departments connection to the SGN and the secure connection to the Internet, as well as provide the initial Help Desk and support capability to manage any problems arising. The Operations Centre will also be the first line of contact between the Government SGN users and JTC. To ensure the requisite levels of availability regarding the Operations Centre services there will be a need for full resilience to be built within the solution, as well as a full disaster recovery plan in the event of uncontrollable loss of the prime Operations Centre.

3.2 Connection Requirements

3.2.1 Introduction

The SGN's data interfaces to the network carrier shall occur at routers that are either, owned by the GOJ's e-Government Department or leased from JTC, and operated and managed at the e-Government SGN Operations Centre on behalf of the Government. e-Government should also consider the option of introducing a 'subscription model' as an alternative means of spreading the budgetary requirement. (i.e. Each institution pays a subscription charge). The connection point linking a department to the SGN shall be of a standard implementation, each access point to the SGN shall have a router and firewall element.

The local connectivity to the departments shall be made via a limited family of router devices. The routers shall be capable of supporting from 64Kbps up to 155Mbps. These routers will be located in the premises of the user organisations. To ensure the security and integrity of both the SGN and departmental networks, a firewall service shall be located behind every access router. To increase the level of security the firewall and router solutions should be from alternate product ranges and should have a history of being delivered together under a single implemented solution.

3.2.2 Requirements of Connected Organisations

Certain criteria should be met before any given ministry should be allowed connection to the SGN.
It is apparent from our visits to the various organisations that, in general, LAN administrators are not fully documenting their procedures and Inventories.
As a pre-requisite to joining the SGN it is recommended as a minimum that each institution should demonstrate its ability to meet a standard set of requirements that will include:

a) An Address List – A list containing all addresses on the network, including the hardware addresses of all computers. E.g. IP Address, Physical Location, Prime user
b) A network Map – Hardware and cable locations
c) Equipment List – Data of Purchase, serial numbers, operating system, manufacturers etc.
d) Server Configuration – A list of server hardware configuration, software, usage (file server, web server, email, database server, etc) and location of backups.
e) Security – Improve restrictions on access to computers/servers. E.g. Install automatic locks on all server rooms.

3.3 Network management

The e-Government Operations Centre will have prime responsibility for the overall management, configuration and support of the Department connectivity to the SGN physical network. This incorporates both the router and firewall products, their configuration and associated 'move, add, change' mechanisms. In addition the e-Government Operations Centre will have the responsibility for configuration and management of the Internet 'demilitarised zone' (DMZ) that will provide the secure connection to the Internet for all e-services.

The Operations Centre will also be expected to develop and manage the relationships with all identified product suppliers, so as to more easily support the Help Desk function in problem resolution.

The configuration of the departmental routers and firewalls will play a major role in the connectivity capability and subsequent management of the Departments connection to the SGN. The routers and firewalls must be both proactively and where necessary reactively managed with regard to their 'well being', availability and performance.

Connectivity to the SGN, via the router and firewall, will incorporate a range of services including:

- Network Address Translation,
- Quality of Service,
- Virtual Private Network,
- Domain Naming Service and overall management and monitoring of the SGN connectivity devices.

These will form part of the e-Government Operations Centre responsibility. Processes will need to be developed to describe how the Operations Centre will provide these services and how it will interface with the

connected institutions regarding issues such as any implementation or amendment that impacts their internal configurations and services.

3.3.1 Network Management Requirements

1. The SGN Design shall provide details on what tools, processes and mechanisms that will need to be utilised to enable the successful remote management and configuration of the routers, firewalls, the DMZ and the services implemented to provide the end-to-end SGN service infrastructure. This will include:
    a. Detailed definition of the system management tools utilised to remotely manage the firewalls and routers and the infrastructure architecture within which they run.
    b. Details regarding the protocols utilised to mange the routers and firewalls and the levels of managed available within the associated MIBs.
    c. Details of how alerts generated by the firewalls and routers will be prioritised and how the identification of an alert will be passed to the requisite 2nd line support agent.
    d. Details of what processes will be put in place to remotely manage the firewalls and routers, using what security mechanisms and audit trails.
    e. Details of how the configurations and operating systems of the routers and firewalls will be maintained and through what tools.
    f. Details of how the audit information will be secured and made available for any subsequent independent review.
    g. Details on how the routers will be configured and maintained to support the IPSec protocol for VPN tunnelling across the SGN.
    h. If appropriate, details of how the remote management of keys in support of IPSec. Tunnelling will need to be implemented and subsequently managed.
    i. If appropriate, details of how the introduction and subsequent management of any security policy server and the certificate server in support of VPN tunnelling will be implemented.
    j. Details of what form of router-based VPN service will be implemented (software or on-board processing).
    k. Details of what assistance the GOJ will require in defining and setting up a government wide naming structure that will be used by the DNS hierarchy to identify the corporate services e.g. email and Portal/Gateway within the SGN environment.
    l. Details of how a Domain Naming Service will be implemented to support the use of shared services, Department to Department and Portal/Gateway to Department interaction, plus how this will interface with the DNS services already supported by the existing Department IP infrastructures
    m. Recommendations in regard to any DNS caching and the 'time to live' value, especially within any Departmental DNS service.
    n. Details of how any future Quality of Service (QoS) functionality will be implemented, configured and maintained on the routers.
    o. Details of how they will consider setting up a network policy server and how this will be utilised in the QoS service and through what protocol.
    p. Details how they will manage the promulgation of the QoS requirements into the JTC switched fabric and ensure maintenance of the QoS and associated policies.
    q. Details of how Network Address Translation will be applied at the router boundaries for internal and external traffic. The SGN will utilise a common IP addressing structure and the router will provide the necessary IP translation. The e-Government Operations Centre will detail how it will manage, configure and monitor the NAT environment.
    r. Details of how the e-Government Operations Centre will set up a process for managing the changes within the SGN IP structure and the relationship with any changes within internal Departmental IP structures that impact the NAT service.

2. The SGN Design shall detail recommendations on controlling the segmentation of bandwidth throughput at the Internet connection, based upon policy decisions associated with each participating Departments Internet needs. Plus how this bandwidth segmentation will be managed as to its utilisation and potential change.

3. The SGN Design shall provide details of how to implement a 'Implement, Move, Add, Change' process for the SGN connections. It should detail the processes and mechanisms used by the Department to request an IMAC, and how the e-Government Operations Centre will subsequently manage the

processes. It should also include provisional timings associated with the IMAC process and what responsibilities are required of the requesting Department.

A key component within the Network Management is the 'management' of the telecommunications supplier (JTC) with regard to the service availability and provision. Any problems identified will be passed on to the Help Desk for subsequent management. A process will be implemented enabling the Network Management staff to have the requisite 'view' of the telecommunications suppliers service characteristics such that when problems occur or are identified as 'potential problems' the e-Government Operations Centre can be informed and any necessary preventative or end user management actions can be undertaken.

4. The SGN Design shall detail the approach needed to set up and subsequently manage the relationship with the telecommunications supplier.

5. The SGN Design shall detail the expected mechanisms for obtaining access to the internal management information generated by the telecommunications supplier's management capability, e.g. availability of switches, knowledge of performance with the network etc.

6. The SGN Design shall detail what information should be anticipated from the telecommunications supplier to enable the e-Government Operations Centre to provide the expected level and quality of service and support. To enable the above to be successful recommendations are required on how to engender a close and mutually beneficial relationship with JTC.

7. The SGN Design shall include a preferred approach to the development of an interface and subsequent management of the other third-party suppliers e.g. router and firewall.

8. The SGN Design shall detail what levels of resilience will to be incorporated within the e-Government Operations Centre so as to ensure the availability of the e-Government Operations Centre environment and ensure the ability to continue remote management of the services within its responsibility, based on an availability agreement of 99.8%.

9. The SGN Design shall include details regarding the recommended approach to any backup and restoration of data/databases that is deemed essential to both ensure the integrity of the e-Government Operations Centre environment, the services it supports and also to comply with any IT Security Policy directives e.g. back-up of audit files, back-up of configuration details to enable speedy recovery etc.

10. The SGN Design shall define the processes and procedures that will need to be put in place to ensure the security and integrity management of the back-up data itself.

3.4 Additional Network Services

It is possible that additional corporate services will be introduced over time and that these services will connect to the SGN, via the standard secure connection, and will be accessible by all Government end-users. These services will include email, Intranet, Central enterprise Directory etc. It is intended that these services will be managed by the Operations Centre and the processes and procedures agreed for the connectivity to the SGN be expanded to encompass the additional services. The impact of these services may result in increased Operations Centre availability and responsibility.

11. The SGN Design shall detail recommendations on how the Operations Centre could be scaled to support these additional services, identifying what changes will be necessary to the people, tools, processes and procedures put in place for the 'original Operations Centre'.

3.4.1 Email

One of the main uses of the SGN is to promote electronic communication between the various institutions. As such it is essential that a standard messaging system be introduced across all connected parties. It is recommended that this messaging system is located and managed centrally. An investigation into the implementation of a corporate messaging system is covered to a separate statement of work. The results of the investigations are documented in Email Statement of Needs GOJ.CONS.ANLS.028.0.2 Document reference 2.

3.4.2 Intranet and Internet Tracking

12. It is essential that services must be available to monitor and track all usage of the Intranet and Internet. These services shall be managed both centrally and remotely.

3.4.3 Corporate Enterprise Directory

The SGN shall make full use of a corporate enterprise directory.

Requirements relating to this are contained within document reference 2 - Email Statement of Needs GOJ.CONS.ANLS.028.0.2

3.4.4 The SGN & Portal

The final design decisions relating to the GOJ Portal have not yet been made at the time of writing this document. The Portal will not become necessary to the SGN until a large number of GOJ institutions have connected to the SGN. At that point, users would begin to encounter difficulties in finding information, so the Portal would become more necessary. In the first stage of the SGN however, if there are only a few GOJ institutions connected, the SGN could be launched without the Portal.

In time it is anticipated that the GOJ Portal may become the initial reference point for all e-Government users , with comprehensive search facilities. This would be similar to the portal sites that have been implemented by other national governments.

It is currently expected that the GOJ Portal will be implemented in several phases with its functionality being progressively increased with each phase.

3.5 Resilience

The availability of the connection to the SGN and the Operations Centre, including all of its attendant functions, is crucial to the success of the SGN. It is essential that the connections to and the provision of the SGN service (by JTC) is monitored and maintained on a par with the levels to be agreed with JTC i.e. 99.8% (minimum). This requires in-built resilience to be incorporated in all architectures, designs and implementations. This resilience will need to be identified and demonstrated.

13. The SGN Design shall include details of the levels of redundancy and resilience that should be implemented as part of the Department to SGN connectivity (router and firewall). This should include local LAN connectivity, firewall resilience and router resilience. Approaches and their associated costs and risks should also be provided.

14. The SGN Design shall included details of the recommended approach to resilience within all the functions incorporated within the Operations Centre. Recommendations regarding this resilience should include, but not be limited to:

    a. The level and type of resilience required within the hardware/software infrastructure used to support the system management capability (at all levels, including network and hardware management as well as firewall and service management)
    b. The level and type of resilience required within the hardware/software infrastructure used to support the Help Desk function
    c. The level of resilience required with the Operations Centre network infrastructure
    d. The level of resilience required in any network connectivity to 2nd and 3rd line support services/staff
    e. The level of resilience required within the Operations Centre environment e.g. power supply, air conditioning etc.
    f. The approach needed to data back-up and recovery and how backed-up data should be stored
    g. The processes and mechanisms needed to manage and support the delivery of a resilient infrastructure and service
    h. Details regarding any degradation in the service that could be introduced should any level of resilience be invoked
    i. Details of the required processes that will be need to be invoked to rectify any occurrence of a resilient factor such that the full levels of resilience are restored as soon as is practicable

3.6 Security

3.6.1 Security Management

The e-Government Operations Centre has a responsibility within the overall Accreditation process for secure connectivity to the SGN. The Accreditation process will be owned by the Government and will incorporate the reviewing of existing Departmental network and security mechanism to ensure that they will not compromise the overall security and integrity of the SGN and the Departments connected. The e-Government Operations Centre will be required to provide assistance regarding any network related issues and questions. It will also be part of the overall 'end to end' security mechanism, in-line with the Government's IT Security Policy, with regard to the configuration and management (physical and process related) of the firewalls utilised.

The e-Government Operations Centre will also have the task of configuring and managing the Internet DMZ. The DMZ will provide a high security environment with multiple levels and types of security capability to ensure both the integrity of all services being provided for Internet utilisation as well as the over all integrity of the SGN and its connected Departments.

Both the connection to the SGN and the DMZ will utilise products, protocols and services that conform to the GOJ IT Security Policy.

3.6.2 Security Management Requirements

15. The SGN Design shall include the tools, processes and procedures required to provide the implementation, configuration and management of the firewalls and DMZ components.

16. The SGN Design shall include information regarding how the security integrity of both the firewall/DMZ and the network should be maintained. This should also address recommended levels of intrusion detection capability at both the perimeter and internally within the SGN.

17. The SGN Design shall recommend the provision of audit information, format, level and recommended tools.

18. The SGN Design shall recommend a method to allow the Operations Centre to support the Accreditation Process.

3.6.3 Security of Network

3.6.3.1 Routers

19. The SGN Design shall provide recommendations regarding the audit processes required to ensure the security and integrity of the Departmental connections, including any tools, processes and levels of audit information, plus details of how long the information should be maintained.

20. The SGN Design shall recommend a process whereby Government security representatives could be able to access and audit the information and processes utilised by the SGN Design.

21. The SGN Design shall recommend provision of hardened authentication control features on the selected router solution/s.

22. The SGN Design shall recommend secure processes and procedures for the management of the selected router solution/s passwords and access control. For example, using the same community strings for all network devices should be avoided.

23. The SGN Design shall recommend a method of ensuring secure processes and procedures for interactive access control to the selected router solution/s.

24. The SGN Design shall recommend an approach regarding the logging capabilities of the selected routers and their usage. A further recommendation should be made on the potential use of these logging capabilities.

25. The SGN Design shall recommend a full range of security features and associated functionality that will be required as part of the provision of a router service.

3.6.3.2 Firewall

26. The SGN Design shall ensure that the firewall solution/s identified is Common Criteria EAL4 level or ITSEC E3 level compliant as per standards dictated by the GOJ IT Security Policy.

27. The SGN Design shall define the most effective configuration set-ups for each of the firewall implementations.

28. The SGN Design shall detail how full authentication would be ensured for all administration.

29. The SGN Design shall recommend the required levels of security regarding any remote administration.

30. The SGN Design shall recommend processes and mechanisms will be need to be put in place to ensure the security and integrity of all the routers and firewalls located at remote Department locations.

3.6.3.3 Internet Boundary Security

With the provision of a Government-wide network infrastructure that will enable the introduction of any-to-any communication between Government Departments and communication with external entities (e.g. citizens,

businesses, suppliers etc.) comes the need to provide a fully secure and managed service to control and support the connectivity from this new network to the public Internet.

Utilisation of this connectivity to the Internet can be for a range of reasons, including end-user access to Internet services through to e-enabled integration of services and systems. However, the Internet as a whole is not trustworthy, and as such those organizations connecting to the Internet are putting their internal systems and networks in a vulnerable position, open to potential misuse and attack. To combat this the concept of an Internet Gateway or DMZ, as it is often known, has been developed.
Perimeter security is a major consideration for any e-Government network infrastructure. Because the nature of an e-Government network is to conduct service transactions for all citizens, residents and businesses under its governance, it becomes a likely target for malicious activity originating from the Internet community at large. Consequently the architecture must provide the requisite security capability to meet the requirements of the GOJ Internet Gateway.

31. The SGN Design shall detail the technologies, responsibilities, mechanisms and processes associated with providing the SGN with secure connectivity to the public Internet. The Internet boundary security (DMZ) would provide the central point of access into and out of the SGN to the Internet. The extent of this requirement is bounded by the extent of the DMZ, thus internal security of the SGN is outside the scope of this particular requirement, as are any other external connections to the SGN. Such connections, if they exist, shall either be removed or assessed (and secured) in a similar way to that documented here and shall fall under the remit of the GOJ.

32. The eventual SGN provider shall agree to have, on an agreed frequency between themselves and the Government, independent accreditation (primarily through a series of managed and controlled attempts at breaching the security, via a range of mechanisms and approaches), so as to ensure the integrity and capability of the perimeter security installations.

3.6.3.4 Internet Service Provider

Currently the various institutions visited use a number of different Internet Service Providers (ISP). In the main NIC is the ISP for the majority of government organisations and many non-government organisations. This monopoly diminished due to the advent of numerous new licences service providers. The e-Government team needs to make a decision on whether a single ISP should be used across the SGN or multiple ISP's utilised. It should be borne in mind that a single ISP would minimise the firewall requirements whilst maximising the risk of Internet access failure. It should also be noted that to enforce a single ISP across NMIs might prove unrealistic. This may be particularly important if the chosen ISP provides a service level below existing service levels and/or links. E.g. Central bank has a 2Mb linked with NIC at present. In phase one of the SGN rollout it is recommended that NIC be used as the ISP.

33. The SGN Design shall recommend an approach, which allows an eventual combination of multiple Internet access methods.

3.6.3.5 Remote Access Service

The users of the SGN shall in the long term have a requirement for remote access to the SGN. Remote access is a method for the providing travelling or homebound users with access to the voice and data networks of the GOJ. The predominant method of providing remote access is through telephone lines on the public network. Telephone lines are ubiquitous and provide a reliable circuit for low speed data traffic. The GOJ wishes to introduce a centralised remote access service that shall control external connections to internal department networks via a single point of entry through the SGN. The SGN Design shall detail a recommended solution.

34. The SGN Design shall support a unique remote access ID per each single user and ensure that every unique remote access ID can only support a single active session.

35. The SGN Design shall ensure the remote access service's toolset supports a mechanism that enables the management of any prescribed GOJ password policy e.g. password expirations of inactive accounts, password quality controls, password aging, password history etc.

36. The remote access service recommended must support automatic disconnection of sessions inactive after a given period of time i.e. timing out inactive sessions.

37. The remote access server recommended must support multiple privilege user levels, e.g. separate administrative passwords.

38. The remote access service recommended must support the logging of successful connections and failed events. Activity logs must record the date and time of the event, record user Ids and must record the success or failure of the event. The activity logs must also be protected from unauthorized access. The generation of real time alarms, e.g. SNMP traps, should be supported that can handle and detect anomalous or suspicious events.

39. The SGN Design shall also indicate if any recommended product is capable of integrating with any standard enterprise management solutions, such as HP Openview, CA Unicenter, or Tivoli.

40. The remote access service must initially support up to 500 concurrent connections.

41. The remote access service must have an authentication mechanism in place to verify the identity of each user. The SGN Design shall recommend an authentication mechanism.

42. All authentication data must be stored in encrypted format; the SGN Design should recommend a form of authentication data storage and how the authentication data would be secured.

43. The remote access service must support encrypted communications. All remote access sessions are to be conducted via the Internet and/or via dial-up, the remote access service must support encryption of sessions across the Internet and/or the public telecommunications network. The remote access server must support both ISDN and modem connectivity if a dial up service is provided. The modem card software should be upgradeable if necessary, to enable the support of new standards, such as the upgraded V.90 standard, V.92. The SGN Design shall recommend the type of encryption to could be implemented.

44. The SGN Design shall detail throughput limit (e.g. bandwidth).

45. The SGN Design should also recommend additional features of any proposed remote access solution such as:
    a. Automatic dial back
    b. Provision of file transfer crash recovery
    c. Support data compression

3.7 Scalability

It is essential, both to the overall success of the SGN and limiting the initial start-up costs, that the initial implementation of the SGN and the connected institutions is of a manageable size. However the overall goal is to connect all 103 GOJ institutions and potentially many more NMIs. With this in mind it is imperative that:

46. The SGN Design shall include highly scaleable network Equipment.

47. The SGN Design allows easy incorporation of additional connections and associated equipment.

4 Phasing

The intent within the GOJ is that eventually all government institutions will be connected to the SGN. A number of targeted institutions will be connected before end 2002. As such each institution will require the installation and configuration of the requisite routers and firewalls. The 18 institutions targeted for connection in phase 1 are shown in the table below (A equates to a high level of criticality, B equates to a medium level of criticality, C equates to a low level of criticality). All connections will utilise 128Kbps ISDN connections as back-up. The Operations Centre (not shown) will be dual 155Mbps and Internet connectivity (not shown) will be 34Mbps with 2Mbps back up. (These figures should be used as estimates). Assuming the network scalability requirements are met it may be financially prudent to start with 512kbs, monitor the traffic flows closely for 3-6 months and up the bandwidths if required.

Department Name	Bandwidth Requirement	Category
Ministry of Finance (MoF)	> 1Mbps. (up to 34 Mbps.)	A
Ministry of Industry and Trade (MIT)	> 1Mbps. (up to 34 Mbps.)	A
Ministry of Information, Communications & Technology (MoICT)	> 1Mbps. (up to 34 Mbps.)	A
Ministry of Planning (MoP)	> 1Mbps. (up to 34 Mbps.)	A
Ministry of Public Works and Housing (MoPW)	> 1Mbps. (up to 34 Mbps.)	A
Municipality of Amman (MoGA)	> 1Mbps. (up to 34 Mbps.)	A
National Information Centre (NIC)	> 1Mbps. (up to 34 Mbps.)	A
Prime Minister's Office (PM)	> 1Mbps. (up to 34 Mbps.)	A
Capital Markets (part of MoF)	2Mbps.	B
Central Bank (CBJ)	2Mbps.	B
Customs (part of MoF)	512Kbs	B
Dept of Social Security (DSS)	512Kbs	B
Jordan Export Development (JEDCO)	512Kbs	B
Jordan Industrial Estates (JIEC)	512Kbs	B
Jordan Investment Board (JIB)	512Kbs	B
Aqaba free Zone (ASEZA)	512Kbs	C
Department of Statistics (DoS)	512Kbs	C
National Library (part of Ministry of Culture)	512Kbs	C

4.1 Rollout Requirements

48. The SGN Design shall outline the processes required to select, implement and configure the requisite firewalls and routers within each Department.

49. A preliminary list of requirements will been sent to the Ministries. The SGN Design will supplement this by the inclusion of a list of the information required from the Departments with regard to supporting a successful rollout, including what lead time will be required regarding any 'surveys' of target Departments.

50. The SGN Design shall recommend procedures required to manage any necessary changes in Department connections/equipment room environment to support the successful implementation.

51. The SGN Design shall include a 'first draft' implementation plan showing how best to successfully connect the identified Departments to the SGN, based on the high-priority/low-priority table above.

52. The SGN Design shall recommend the processes will be need to be in place with regard to the management of any subsequent 'move, add, change' process for SGN connectivity, including timeframes and responsibilities.

5 Technical Requirements

5.1 General Router and Firewall Requirements

53. The firewall and router solution shall support the availability target of the SGN, which is 99.8%.

54. The firewall and router solution shall facilitate the centralised management of all the distributed firewall and router elements. Details of supported protocols and management capability are required, including the ability to interface with industry standard network management tools.

55. The firewall and router solution shall provide a range of performance levels, for traffic throughput within the SGN, from 64kbps up to 155Mbps on the external side to the department. The SGN Design shall include information on the following:
    a. Packet throughput.
    b. Encryption throughput (router only).
    c. Percentage package loss.
    d. Latency, i.e. ms per hop.

56. The firewall and router solution shall support a strong security logging capability and log file analysis with report generation also required. It could be a 3rd party product that interfaces with the firewall completely so both solutions should incorporate a high degree of interoperability.

57. The firewall and router solution shall ensure that a stream of remedial updates or patches is made available to ensure the solution's long-term effectiveness.

58. The recommended firewall and router solution should have been deployed in a number of previous implementations, preferably within government and are referenced.

59. The introduction of the firewall and router solution and any associated tunnelling or access negotiation facilities shall not cause unintended failures of legitimate and standards-compliant usage that would work were the firewall not present.

60. The SGN Design shall include details of the firewall and router solution's resilience and Mean Time Between Failure (MTBF).

61. The SGN Design shall include details of the fail-over functionality of the firewall and router solution. The fail-over SGN connection shall be provided by ISDN, details are required of the procedures involved when a failure occurs (ATM to ISDN) and when a resumption of service occurs (ISDN to ATM).

62. The SGN shall have a complete set of documentation to support the implementation of the firewall and router selection.

5.2 Routers

63. The router solution/s identified shall be available as a family of devices detailing performance, scalability and limitations.

64. The router solution/s identified shall be capable of supporting a range of connectivity such as "E3, STM4 and ISDN" (external – fibre and copper) and a range of internal LAN/SGN connectivity such as gigabit Ethernet.

65. The router solution/s identified shall support the use of Access Control Lists (ACL) to permit or deny connections based on protocol, services, application or IP addresses.

66. The router solution/s identified shall be ATM capable.

67. The router solution/s identified shall be capable of interacting with and be configured by the SNMP network management systems for basic functions.

68. The router solution identified with the identified Network Management System (NMS) shall be able to interact accurately with SNMP using both IETF and proprietary Management Information Bases (MIB's).

69. The routers solution/s identified shall be capable of sending traps and the NMS must capable of processing the trap and performing a pre-defined task.

70. The router solution/s identified shall be capable of supporting at least two levels of access with appropriate levels of access to the command interpreter.

71. The router solution/s selected shall be able to support a variety of bandwidth requirements from 64kbs up to 155MBs.

72. The router solution/s selected shall support the complete breadth of Quality of Service (QoS) functionality, i.e. latency, jitter, bandwidth, packet loss and availability. A detailed explanation of how this service is to be implemented shall be provided to address this issue.

73. The router solution/s identified shall be IPSec capable networking equipment.

74. The router solution/s identified shall support a Virtual Private Network (VPN) facility and details should be available as to how this service would be provided.

5.3 Firewall Requirements

75. Details and types of connections supported by the identified firewall solution/s for LAN connectivity, e.g. 10 Mbps. 100 Mbps, UTP and fibre shall be provided.

76. The types of functionality of firewall service and associated throughputs should be provided.

77. The firewall solution identified shall support the following protocols – FTP, Telnet, SSL, SMTP, DNS, HTTP, etc.

78. The firewall solution identified shall be fully transparent to end-users.

5.4 Bandwidths & Traffic

The current analysis estimates that at the outset the SGN will only need to support minimum traffic. This is due to the current lack of data sharing and applications that allow inter institutional workflow. The web Applications document identifies numerous applications that will encourage increased usage and therefore greater traffic. This will obviously lead to a requirement for higher levels of bandwidth.

79. The SGN Design shall incorporate recommendations on redundancy and associated mechanisms.

5.5 Routing Protocol, IP Address and DNS Planning and Design

IP address planning, subnet planning and impact on routing protocol selection are the primary focus of this service. Further, issues related to an enterprise DNS services and implementation of the primary DNS servers will need to be addressed as well.

80. The SGN Design shall incorporate details of

    a. Plan and Design the routing protocol to be implemented
    b. Plan for the allocation of registered CIDR block of Class 'C' or Private IP addresses obtained by e-Government.
    c. Plan IP address subnets, and determine its impact on routing protocol selection.
    d. Develop guidelines for the allocation of IP subnets.
    e. Investigate and document issues related to enterprise DNS servers.
    f. Plan and design DNS structure.

5.5.1 Information Prerequisites to Delivery

The following information will be made available to the SGN implementer.

- Information on current allocation of IP addresses(which may be fake), including subnet information.
- Information on total number of IP hosts (current and future), geographical and organizational structure. This will be included in the inventory (still to be done).

5.5.2 The e-Government Resource Commitments

- Active participation by Network and System Administrators.
- e-Government to obtain registered Class 'C' IP addresses or use Private IP addresses or an equivalent.

5.5.3 Deliverables

- Routing Protocol design document
- IP Allocation document, which includes subnet information and guidelines for allocation of subnets.
- Migration plan.
- Enterprise DNS design document.

5.6 Network Design

Whilst not attempting to influence the design of the network, it is believed that the design should be based on a mesh like topology. That is to say that there should be no single point of failure and all institutions shall be capable of communicating directly with all other institutions. This should be without the drawback of normal private mesh topologies which usually means n*(n-1)/2 cables. See below as an example

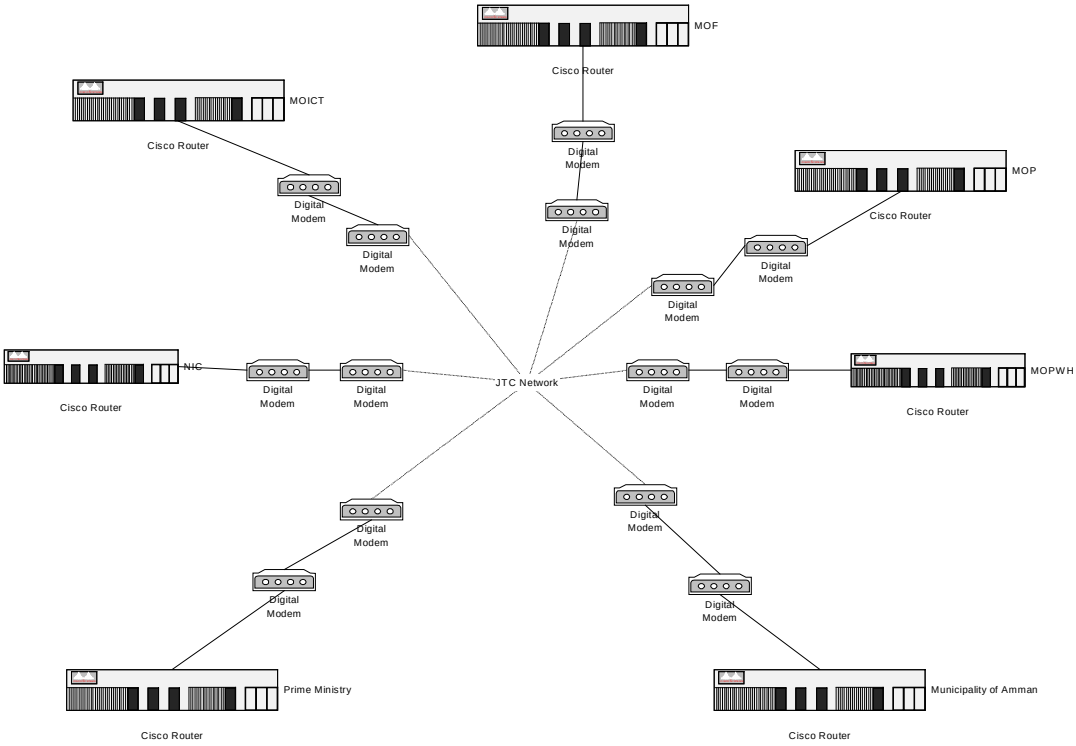

Figure 3 Expected Design Topology

6 Warranty/Support/Maintenance

All network management, active and support components and associated software shall carry a comprehensive warranty period that starts from the installation date and shall extend for a minimum of 12 months from the final component installation. During the warranty period, these components shall be maintained on-site by the SGN at no additional cost to the GOJ.

81. The eventual SGN implementer, in addition to JTC, shall be required to provide appropriate support to the network management, active and support components and associated software and shall be prompt in responding to any call or request made by GOJ staff. The downtime of any access routers or firewalls shall be limited to a maximum of 1 hour during core business hours (Sunday – Thursday 6:30 to 1530) and 4 hours at all other times, after which penalties will be implemented.

A Service Level Agreement covering the network management, active and support components and associated software, with the terms and conditions mutually agreed on during the negotiation period, shall be signed within 12 months of the Contract Completion Date and remain valid for a period of one year which is automatically renewable on annual basis for a further period of seven years unless the GOJ informs the contractor in writing, to the contrary allowing at least thirty calendar days notice.

The SGN implementer shall deliver each network management, active and support components and associated software along with one set of original copies of the complete documentation for that product in hard copy format, and one set of complete documentation in electronic format (CD etc.). The complete documentation shall include user documentation, reference manuals, installation and reconfiguration manuals as applicable, any available charts or diagrams for user's aid, and useful descriptive materials.

Support and Special Conditions

Should a major network management, active and support component fail to operate adequately on or after installation due to lacking module(s) not detected during initial installation by the bidder etc., then the latter shall promptly undertake to replace the component at no additional charges to the GOJ and within one calendar week from the date of notification.

Should any network management, active and support component grossly fail (i.e. recurrent failure of equipment occurring in closely spaced intervals of time), which the SGN implementer fails to rectify within a reasonable period of time despite repeated attempts, the GOJ shall have the right to request proper and complete replacement of the defected component.

7 Training/Education

The GOJ has a clear and well-established intention to invest in its human resources through training, knowledge transfer and hands-on experience. Accordingly, the SGN implementer will be required to provide comprehensive training for IT management and staff on the user, administration and operational support aspects of the proposed technical infrastructure components.

82. The SGN Implementer shall be required to provide details of all training that may be provided to instruct government of all facets of the solutions that would be provided by the SGN implementer. These should include training plans, courses and schedules.

8 Assumptions

1. All institutions connected are responsible for the administration and maintenance of servers on their internal LANs and the LANS themselves.
2. The initial 18 Institutions will start with a minimum of 512Kb connection.
3. The NIC will be the initial ISP for all connected Ministries
4. All 18 institutions will be considered for budget estimates
5. Email will be run centrally from the Operations Centre
6. The SGN availability should be 99.8%
7. JTC provide the ATM backbone

9 Other Information

During our investigations a number of institutions have been identified as being candidates for early connection to the SGN. These institutions should be considered as prime choices for connection in the second phase of the SGN rollout.

The Customs Department has been highlighted in the Web Applications Assessment GOJ-CONS-ANLS-025-0.4a as a government institution whose connection to the SGN would deliver significant benefits (in terms of cost and efficiency improvements) to GOJ through optimisation of the processes related to importing and exporting goods. The Customs and related institutions that should be considered for the second phase of connection to the SGN should consequently include:

- Customs Aqaba (because it is a major transit point and therefore very busy)
- Customs Jabar
- Customs Omari
- Amman Customs HQ
- Amman Customs House
- Airport Customs House (especially important because importers pay a premium to move goods by air and so will increasingly demand faster clearance)
- Ministry of Health (a major stakeholder in the clearance of goods)
- Ministry of Agriculture (a major stakeholder in the clearance of goods)
- The Military Security Directorate (who provide clearance for electronic equipment).

The Customs Department is also the prime source of critical data - trade statistics - to GOJ. There is clear potential to use the SGN intranet to make trade statistics available to OGDs on a real-time basis. The following GOJ institutions are currently using less efficient dial-up connections to collate this information:

- Ministry of Industry & Trade
- Income Tax Department
- Department of Statistics
- Audit Bureau
- Ministry of Agriculture
- Agricultural Marketing Institution
- Ministry of Health
- General Sales Tax Department.

(The Ministry of Industry & Trade and the Department of Statistics are already under consideration for connection to the initial SGN).